Prescribing valuations of the order of a point in the reductions of abelian varieties and tori

Antonella Perucca

Abstract

Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point on G of infinite order. Call n_R the number of connected components of the smallest algebraic K-subgroup of G to which R belongs. We prove that n_R is the greatest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. Furthermore, let $m > 0$ be a multiple of n_R and let S be a finite set of rational primes. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every ℓ in S the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ equals $v_\ell(m)$.

1 Introduction

Let G be a semi-abelian variety defined over a number field K. We consider reduction maps on G by fixing a model for G over an open subscheme of $\operatorname{Spec}\mathcal{O}$, where $\mathcal{O}$ is the ring of integers of K.

Remark that different choices of the model may affect only finitely many reductions because in fact any two models are isomorphic on a (possibly smaller) open subscheme of $\operatorname{Spec}\mathcal{O}$.

Let R be a K-rational point on G. For all but finitely many primes $\mathfrak{p}$ of K the reduction modulo $\mathfrak{p}$ is well defined on the point R and the order of $(R \bmod \mathfrak{p})$ is finite. It is natural to ask the following question: how does the order of $(R \bmod \mathfrak{p})$ behave if we vary $\mathfrak{p}$?

It is easy to see that if R is non-zero then for all but finitely many primes $\mathfrak{p}$ of K the point $(R \bmod \mathfrak{p})$ is non-zero. A first consequence is that if R is a torsion point of order n then for all but finitely many primes $\mathfrak{p}$ of K the order of $(R \bmod \mathfrak{p})$ is n. A second consequence is that if R has infinite order then the order of $(R \bmod \mathfrak{p})$ cannot take the same value for infinitely many primes $\mathfrak{p}$ of K. In this paper we prove the following result:

Main Theorem 1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point on G of infinite order. Call n_R the number of connected components of the smallest K-algebraic subgroup of G containing R. Then n_R is the largest positive integer which divides the order of* $(R \bmod \mathfrak{p})$ *for all but finitely many*

primes $\mathfrak{p}$ of K. Furthermore, let $m > 0$ be a multiple of n_R and let S be a finite set of rational primes. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every ℓ in S the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ equals $v_\ell(m)$.

It is interesting to see whether our result generalizes to semi-abelian varieties. In this generality we prove that for every integer $m > 0$ there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the order of $(R \bmod \mathfrak{p})$ is a multiple of m (see Corollary 4.4). Also for all but finitely many primes $\mathfrak{p}$ the order of $(R \bmod \mathfrak{p})$ is a multiple of n_R (see Proposition 2.2).

The Main Theorem and the results in section 4 (Proposition 4.1, Proposition 4.2 and Corollary 4.4) strengthen results which are in the literature: [9, Lemma 5]; [12, Theorems 4.1 and 4.4]; [1, Theorem 3.1] and [2, Theorem 5.1] in the case of abelian varieties. Further papers concerning the order of the reductions of points are [6], [10] and [8].

2 Preliminaries

Let G be a semi-abelian variety defined over a number field K. Let R be a K-rational point on G. Write G_R for the Zariski closure of $\mathbb{Z} \cdot R$ in $G \times_K \bar{K}$ (with reduced structure). Because $\mathbb{Z} \cdot R$ is dense in $G_R(\bar{K})$, it follows that G_R is an algebraic subgroup of G defined over K. In particular for every algebraic extension L of K we have that G_R is the smallest algebraic L-subgroup of G such that R is an L-rational point. Write G_R^0 for the connected component of the identity of G_R. Then G_R^0 is an algebraic subgroup of G defined over K and $G_R^0(\bar{K})$ is divisible. Write n_R for the number of connected components of G_R. The number n_R does not get affected by a change of ground field: since $\mathbb{Z} \cdot R$ is Zariski-dense in $G_R(\bar{K})$ then every connected component of G_R is a translate of G_R^0 by a K-rational point therefore it is also defined over K.

Lemma 2.1. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-rational point on G. Then $G_{n_R R} = G_R^0$. Furthermore, let H be a connected component of G_R. Then there exists a torsion point X in $G_R(\bar{K})$ such that $H = X + G_R^0$.*

Proof. Clearly G_R^0 contains $G_{n_R R}$. Also G_R^0 is mapped to $G_{n_R R}$ by $[n_R]$. Because this map has finite kernel, G_R^0 and $G_{n_R R}$ have the same dimension. Then since G_R^0 is connected, we must have $G_{n_R R} = G_R^0$.

Let P be any point in $H(\bar{K})$. Then $P + G_R^0 = H$. The point $n_R P$ is in $G_R^0(\bar{K})$. Since $G_R^0(\bar{K})$ is divisible, there exists a point Q in $G_R^0(\bar{K})$ such that $n_R Q = n_R P$. Set $X = P - Q$, thus X is a torsion point in $G_R(\bar{K})$. Then we have:

$$H = P + G_R^0 = P - Q + G_R^0 = X + G_R^0.$$

□

Proposition 2.2. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-rational point on G. Then n_R divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K.*

Proof. Because of Lemma 2.1 there exist a torsion point X in $G_R(\bar{K})$ and a point P in $G^0_R(\bar{K})$ such that $R = P + X$. Then clearly $n_R X$ is the least multiple of X which belongs to $G^0_R(\bar{K})$. Call t the order of X. Let F be a finite extension of K where P is defined and $G_R[t]$ is split. Fix a prime $\mathfrak{p}$ of K and let $\mathfrak{q}$ be a prime of F over $\mathfrak{p}$. Call m the order of $(R \bmod \mathfrak{p})$. Up to excluding finitely many primes $\mathfrak{p}$ of K, we may assume that the order of $(R \bmod \mathfrak{q})$ is also m. The equality $(mX \bmod \mathfrak{q}) = (-mP \bmod \mathfrak{q})$ implies that $(mX \bmod \mathfrak{q})$ belongs to $(G^0_R(F) \bmod \mathfrak{q})$. Then $(mX \bmod \mathfrak{q})$ belongs to $(G^0_R \bmod \mathfrak{q})[t]$.

Up to excluding finitely many primes $\mathfrak{p}$ of K, we may assume that the reduction modulo $\mathfrak{q}$ maps injectively $G_R[t]$ to $(G_R \bmod \mathfrak{q})[t]$ and that it maps surjectively $G^0_R[t]$ onto $(G^0_R \bmod \mathfrak{q})[t]$. See [10, Lemma 4.4]. We deduce that mX belongs to $G^0_R[t]$. Then m is a multiple of n_R. This shows that for all but finitely many primes $\mathfrak{p}$ the order of $(R \bmod \mathfrak{p})$ is a multiple of n_R. □

Definition 2.3. Let G be a semi-abelian variety defined over a number field K. Let R be a K-rational point on G. We say that R is *independent* if R is non-zero and $G_R = G$.

By this definition an independent point has infinite order. Notice that this definition does not depend on the choice of the number field K such that R belongs to $G(K)$.

In Remark 2.6 we prove that if G is the product of an abelian variety and a torus then R is independent if and only if it is non-zero and the left $\operatorname{End}_K G$-module generated by R is free. Then rational points of infinite order on the multiplicative group or on a simple abelian variety are independent.

Lemma 2.4. *Let G be a semi-abelian variety defined over a number field K. Let R be a K-rational point on G of infinite order. Then the point $n_R R$ is independent in G^0_R. Furthermore, let X be a torsion point in $G(K)$ and suppose that R is independent. Then $R + X$ is independent.*

Proof. By Lemma 2.1 we have $G_{n_R R} = G^0_R$ therefore $n_R R$ is independent in G^0_R.

For the second assertion, we have to prove that $G_{R+X} = G$. Call t the order of X. Clearly $G_{R+X} \supseteq G_{t(R+X)} = G_{tR}$. Because $G_R = G$ it suffices to show that $G_{tR} = G_R$. Remark that G_R contains G_{tR} and that G_R is mapped to G_{tR} by $[t]$. Because $[t]$ has finite kernel, G_R and G_{tR} have the same dimension. Because G_R is connected it follows that $G_{tR} = G_R$. □

Proposition 2.5. *Let K be a number field. Let $G = A \times T$ be the product of an abelian variety and a torus defined over K. Then a connected algebraic K-subgroup of G is the product of a K-abelian subvariety of A and a K-subtorus of T.*

Proof. Let V be an algebraic subgroup of G. Call π_A and π_T the projections of V on A and T respectively. Remark that $\pi_A(V)$ is a connected K-subgroup of A therefore it is an abelian subvariety of A. Similarly $\pi_T(V)$ is a connected K-subgroup of T therefore it is a subtorus of T. By replacing G with $\pi_A(V) \times \pi_T(V)$, we may assume that $\pi_A(V) = A$ and $\pi_T(V) = T$.

Write $N_T = \pi_T(V \cap (\{0\} \times T))$ and $N_A = \pi_A(V \cap (A \times \{0\}))$. Remark that N_A and N_T are K-algebraic subgroups of A and T respectively. It suffices to show that $N_A = A$ and $N_T = T$ because in that case $V = A \times T$ and we are done. To prove the assertion, we make a base change to $\bar{K}$. Since the category of commutative algebraic $\bar{K}$-schemes is abelian ([7, Theorem p. 315 §5.4 Expose VI_A]) it suffices to see that the quotients $\hat{A} = A/N_A$ and $\hat{T} = T/N_T$ are zero. The quotient A/N_A^0 is an abelian variety (see [13, §9.5]) and then the quotient of A/N_A^0 by the image of N_A in A/N_A^0 is an abelian variety (see [11, Theorem 4 p.72]). Hence $\hat{A}$ is an abelian variety. Because of [5, Corollary §8.5] the algebraic group T/N_T^0 is a torus. The quotient of T/N_T^0 by the image of N_T in T/N_T^0 is an affine algebraic group (see [5, Theorem §6.8]). Hence $\hat{T}$ is an affine algebraic group.

Call α the composition of π_A and the quotient map from A to $\hat{A}$. Similarly call β the composition of π_T and the quotient map from T to $\hat{T}$. The product map $\alpha \times \beta$ is a map from V to $\hat{A} \times \hat{T}$. Now we show that the projection $\pi_{\hat{A}}$ from $\alpha \times \beta(V)$ to $\hat{A}$ is an isomorphism. Clearly $\pi_{\hat{A}}$ is an epimorphism. Since we are working in an abelian category, it suffices to show that $\pi_{\hat{A}}$ is a monomorphism. Because the map $\alpha \times \beta$ from V to $\alpha \times \beta(V)$ is an epimorphism, it suffices to check that the maps $\pi_{\hat{A}} \circ (\alpha \times \beta)$ and $\alpha \times \beta$ have the same kernel. The kernel of the first map is $V \cap (N_A \times T)$. The kernel of the second map is $V \cap (N_A \times T) \cap (A \times N_T)$. We show that these two group schemes are isomorphic because they have the same groups of Z-points for every $\bar{K}$-scheme Z. The Z-points of the first kernel are the pairs (a, b) in $V(Z)$ such that a lies in $N_A(Z)$. Since $(a, 0)$ belongs to $V(Z)$ we deduce that $(0, b)$ lies in $V(Z)$ and so b belongs to $N_T(Z)$. Then the two kernels have the same Z-points. The proof that $\alpha \times \beta(V)$ is isomorphic to $\hat{T}$ is analogous. We deduce that $\hat{A}$ and $\hat{T}$ are isomorphic. Since $\hat{A}$ is a complete variety while $\hat{T}$ is affine the only possible morphism from $\hat{A}$ to $\hat{T}$ is zero. Then $\hat{A}$ and $\hat{T}$ are zero. $\square$

For the convenience of the reader we prove the following remark.

Remark 2.6. Let $G = A \times T$ be the product of an abelian variety and a torus defined over a number field K. Then a non-zero K-rational point R on G is independent if and only if the left $\operatorname{End}_K G$-module generated by R is free.

Proof. The 'only if' part is straightforward: if ϕ is a non-zero element of $\operatorname{End}_K G$ such that $\phi(R) = 0$ then $\ker(\phi)$ is an algebraic subgroup of G different from G and containing R hence containing G_R. Now we prove the 'if' part. Suppose that R is not independent. Because of [14, Proposition 1.5] the left $\operatorname{End}_K G$-submodule of $G(K)$ generated by R is free if and only if the left $\operatorname{End}_{\bar{K}} G$-submodule of $G(\bar{K})$ generated by R is free. Then to conclude we construct a non-zero element of $\operatorname{End}_{\bar{K}} G$ whose kernel contains the point R.

Clearly we may assume that R has infinite order. So G_R^0 is non-zero and since R is not independent we have $G_R^0 \neq G$. By Proposition 2.5, G_R^0 is the product of an abelian subvariety A' of A and a subtorus T' of T. Then either A' or T' are non-zero and either $A \neq A'$ or $T \neq T'$. If A' is zero set $\phi_A = \mathrm{id}_A$, if $A' = A$ set $\phi_A = 0$. Otherwise by the Poincaré Reducibility Theorem there exists a non-zero abelian subvariety B of A such that A' and B have finite intersection and such that the map

$$\alpha : A' \times B \to A \quad \alpha(x, y) = x + y$$

is an isogeny. Call d the degree of α and remark that d is the order of $A' \cap B$. Call $\hat{\alpha}$ the isogeny from A to $A' \times B$ such that $\alpha \circ \hat{\alpha} = [d]$. Call π the projection from $A' \times B$ to $\{0\} \times B$. Set $\phi_A = \alpha \circ [d] \circ \pi \circ \hat{\alpha}$. Remark that if $\alpha(x, y)$ is a point on A' then both x and y are points on A'. Then it is immediate to see that ϕ_A is a non-zero element of $\mathrm{End}_{\bar{K}} A$ and that its kernel contains A'.

If T' is zero set $\phi_T = \mathrm{id}_T$, if $T' = T$ set $\phi_T = 0$. Otherwise, because a subtorus is a direct factor there exists a non-zero ϕ_T in $\mathrm{End}_{\bar{K}} T$ such that T' is contained in $\ker(\phi_T)$. Then by construction $(\phi_A \times \phi_T) \circ [n_R]$ is a non-zero element of $\mathrm{End}_{\bar{K}} G$ whose kernel contains G_R. $\square$

3 The method by Khare and Prasad

In this section we prove the following result, which will be used in section 4 to prove the Main Theorem. To prove this result we generalize a method by Khare and Prasad (see [9, Lemma 5]).

Theorem 3.1. *Let G be the product of an abelian variety and a torus defined over a number field K. Let F be a finite extension of K. Let R be an F-rational point on G such that G_R is connected. Fix a non-zero integer m. There exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R \bmod \mathfrak{q})$ is coprime to m.*

Remark that if $F = K$ the theorem simply says that there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the order of $(R \bmod \mathfrak{p})$ is coprime to m.

Let G be a semi-abelian variety defined over a number field K. For n in $\mathbb{N}$ call K_{ℓ^n} the smallest extension of K over which every point of $G[\ell^n]$ is defined. Let R be in $G(K)$. Then for n in $\mathbb{N}$ call $K(\frac{1}{\ell^n}R)$ the smallest extension of K_{ℓ^n} over which the ℓ^n-th roots of R are defined. Clearly the extensions $K_{\ell^{n+1}}/K_{\ell^n}$ and $K(\frac{1}{\ell^n}R)/K_{\ell^n}$ are Galois.

Lemma 3.2. *Let G be a semi-abelian variety defined over a number field K. Let ℓ be a rational prime and let n be a positive integer. Suppose that $G(K)$ contains $G[\ell]$. Then the degree $[K_{\ell^n} : K]$ is a power of ℓ and for every R in $G(K)$ the degree $[K(\frac{1}{\ell^n}R) : K]$ is a power of ℓ.*

Proof. Since the points of $G[\ell]$ are defined over K, we can embed $\mathrm{Gal}(K_{\ell^n}/K)$ into the group of the endomorphisms of $G[\ell^n]$ fixing $G[\ell]$. The order of this group is a power of ℓ since $G[\ell^n]$ is a finite abelian group whose order is a power of ℓ. Now we only have to prove that the degree $[K(\frac{1}{\ell^n}R) : K_{\ell^n}]$ is a power of ℓ. We can map the Galois group of the extension $K(\frac{1}{\ell^n}R)/K_{\ell^n}$ into $G[\ell^n]$, whose order is a power of ℓ. This is accomplished via the Kummer map

$$\phi_n : \mathrm{Gal}(K(\frac{1}{\ell^n}R)/K_{\ell^n}) \to G[\ell^n]; \quad \phi_n(\sigma)(R) = \sigma(\frac{1}{\ell^n}R) - (\frac{1}{\ell^n}R),$$

where $\frac{1}{\ell^n}R$ is an ℓ^n-th root of R. Since two such ℓ^n-th roots differ by a torsion point of order dividing ℓ^n, it does not matter which root we take. This also implies that ϕ_n is injective. This proves the assertion. □

Lemma 3.3. *Let G be the product of an abelian variety and a torus defined over a number field K. Let R be a K-rational point of G which is independent. Then for all sufficiently large n we have:*

$$K(\frac{1}{\ell^n}R) \cap K_{\ell^{n+1}} = K_{\ell^n}.$$

Proof. Consider the map

$$\alpha_n : \mathrm{Gal}(K(\frac{1}{\ell^{n+1}}R)/K_{\ell^{n+1}}) \to \mathrm{Gal}(K(\frac{1}{\ell^n}R)/K_{\ell^n})$$

given by the restriction to $K(\frac{1}{\ell^n}R)$. To prove this lemma, it suffices to show that α_n is surjective for sufficiently large n.

It is not difficult to check that the following diagram is well defined and commutative (ϕ_n is the Kummer map defined in the proof of Lemma 3.2 and β_n is induced by the diagram):

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Gal}(K(\frac{1}{\ell^{n+1}}R)/K_{\ell^{n+1}}) \arrow[r, "\phi_{n+1}"] \arrow[d, "\alpha_n"'] & G[\ell^{n+1}] \arrow[r] \arrow[d, "{[\ell]}"'] & \mathrm{Coker}\,\phi_{n+1} \arrow[r] \arrow[d, "\beta_n"] & 0 \\
0 \arrow[r] & \mathrm{Gal}(K(\frac{1}{\ell^n}R)/K_{\ell^n}) \arrow[r, "\phi_n"] & G[\ell^n] \arrow[r] & \mathrm{Coker}\,\phi_n \arrow[r] & 0
\end{tikzcd}$$

If β_n is injective then α_n is surjective. Since β_n is surjective, it suffices to prove that $\mathrm{Coker}\,\phi_{n+1}$ and $\mathrm{Coker}\,\phi_n$ have the same order for sufficiently large n. Since the order of $\mathrm{Coker}\,\phi_n$ increases with n, it is equivalent to show that the order of $\mathrm{Coker}\,\phi_n$ is bounded by a constant which does not depend on n. Since we assumed that $G_R = G$, this assertion is a special case of a result by Bertrand ([3, Theorem 1]). □

Lemma 3.4. *Let K be a number field. Let $G = A \times T$ be the product of an abelian variety defined over K and a torus split over K. Fix a rational prime ℓ. If $T = 0$ or if $A = 0$ or*

if ℓ is odd then for every sufficiently large $n > 0$ there exists an element h_ℓ in $\mathrm{Gal}(\bar{K}/K)$ *which acts on $G[\ell^\infty]$ via an automorphism whose set of fixed points is $G[\ell^n]$. If A and T are non-zero and $\ell = 2$ then for every sufficiently large $n > 0$ there exists an element h_2 in* $\mathrm{Gal}(\bar{K}/K)$ *which acts on $G[2^\infty]$ via an automorphism whose set of fixed points is $A[2^n] \times T[2^{n+1}]$.*

Proof. If $T = 0$ then the assertion is a consequence of a result by Bogomolov ([4, Corollaire 1]). If $A = 0$, because T is split over K then it suffices to remark the following fact: for every sufficiently large $n > 0$ the field obtained by adjoining to K the $\ell^{(n+1)}$-th roots of unity is a non-trivial extension of the field obtained by adjoining to K the ℓ^n-th roots of unity. Now assume that A and T are non-zero. Call $\hat{A}$ the dual abelian variety of A. By applying a result of Bogomolov ([4, Corollaire 1]) to $A \times \hat{A}$ we know that if $n > 0$ is sufficiently large, there exists an element h_ℓ in $\mathrm{Gal}(\bar{K}/K)$ which acts on $A \times \hat{A}[\ell^\infty]$ as a homothety with factor h in $\mathbb{Z}_\ell^*$ such that $h \equiv 1 \pmod{\ell^n}$ and $h \not\equiv 1 \pmod{\ell^{n+1}}$. For every n the Weil paring

$$e_{\ell^n} : A[\ell^n] \times \hat{A}[\ell^n] \to \mu_{\ell^n}$$

is bilinear, non-degenerate and Galois invariant. Since e_{ℓ^n} is bilinear and non-degenerate its image contains a root of unity ζ of order ℓ^n. Choose $X_1 \in A[\ell^n]$, $X_2 \in \hat{A}[\ell^n]$ such that $e_{\ell^n}(X_1, X_2) = \zeta$. By Galois invariance and bilinearity we have:

$$\sigma(\zeta) = \sigma\big(e_{\ell^n}(X_1, X_2)\big) = e_{\ell^n}(\sigma(X_1), \sigma(X_2)) = e_{\ell^n}(h \cdot X_1, h \cdot X_2) = \zeta^{h^2}.$$

Because ζ generates μ_{ℓ^n} then σ acts on μ_{ℓ^n} as a homothety with factor $h^2 \pmod{\ell^n}$. Clearly $h^2 \equiv 1 \pmod{\ell^n}$ and $h^2 \not\equiv 1 \pmod{\ell^{n+1}}$ if ℓ is odd. If $\ell = 2$ and $n > 1$ then $h^2 \equiv 1 \pmod{2^{n+1}}$ and $h^2 \not\equiv 1 \pmod{2^{n+2}}$. Because T is split over K we deduce the following: if ℓ is odd the set of fixed points for the automorphism of $G[\ell^\infty]$ induced by h_ℓ is $G[\ell^n]$; if $\ell = 2$ the set of fixed points for the automorphism of $G[2^\infty]$ induced by h_2 is $A[2^n] \times T[2^{n+1}]$. □

Proof of Theorem 3.1. By Proposition 2.5, G_R is the product of an abelian variety A and a torus T defined over F. Let R' be a point in $G_R(\bar{F})$ such that $2R' = R$. Since R is independent in G_R, the point R' is independent in G_R. Call S the the set of the prime divisors of m. Let K' be a finite extension of F over which R' is defined, over which T is split and over which $G_R[\ell]$ is split for every ℓ in S. Apply Lemma 3.3 to the point R', the algebraic group G_R and with base field K'. Then for all sufficiently large n and for every ℓ in S the intersection of $K'(\frac{1}{\ell^n}R')$ and $K'_{\ell^{n+1}}$ is K'_{ℓ^n}. Apply Lemma 3.4 to G_R with base field K': we can choose $n > 0$ such that the previous assertion holds and such that for every ℓ in S there exists h_ℓ as in Lemma 3.4. Call L the compositum of the fields $K'(\frac{1}{\ell^n}R')$ and the fields $K'_{\ell^{n+1}}$ where ℓ varies in S. By Lemma 3.2, the fields $K'(\frac{1}{\ell^n}R') \cdot K'_{\ell^{n+1}}$ where ℓ varies in S are linearly disjoint over K'. Then we can construct σ in $\mathrm{Gal}(L/K)$ such that for every ℓ in S the restriction of σ to $K'(\frac{1}{\ell^n}R')$ is the identity and such that the restriction to $K'_{\ell^{n+1}}$ of σ and of h_ℓ coincide.

Let $\mathfrak{p}$ be a prime of K which does not ramify in L and such that there exists a prime $\mathfrak{w}$ of L which is over $\mathfrak{p}$ and such that $\mathrm{Frob}_{L/K}\,\mathfrak{w} = \sigma$. By Chebotarev's Density Theorem there exists a positive Dirichlet density of prime ideals $\mathfrak{p}$ of K which satisfy the above conditions. Let $\mathfrak{q}$ be the prime of F lying under $\mathfrak{w}$. Fix a prime ℓ in S and suppose that the order of $(R \bmod \mathfrak{q})$ is a multiple of ℓ. Up to discarding finitely many primes $\mathfrak{p}$ the order of $(R \bmod \mathfrak{w})$ is a multiple of ℓ. Let Z be an element of $G_R(L)$ such that $\ell^n Z = R'$. Then the order of $(Z \bmod \mathfrak{w})$ is a multiple of ℓ^{n+1} (respectively of ℓ^{n+2} if $\ell = 2$). Let $a \geq 1$ be such that the order of $(aZ \bmod \mathfrak{w})$ is exactly ℓ^{n+1} (respectively ℓ^{n+2} if $\ell = 2$). Up to discarding finitely many primes $\mathfrak{p}$ there exists a torsion point X in $G_R(L)$ of order ℓ^{n+1} (respectively ℓ^{n+2} if $\ell = 2$) and such that $(aZ \bmod \mathfrak{w}) = (X \bmod \mathfrak{w})$. See [10, Lemma 4.4].

Up to excluding finitely many primes $\mathfrak{p}$, the action of the Frobenius $\mathrm{Frob}_{L/K}\,\mathfrak{w}$ commutes with the reduction modulo $\mathfrak{w}$ of G hence we deduce the following: the point $(Z \bmod \mathfrak{w})$ is fixed by the Frobenius of $\mathfrak{w}$ while $(X \bmod \mathfrak{w})$ is not fixed. Then the point $(aZ \bmod \mathfrak{w})$ is fixed by the Frobenius of $\mathfrak{w}$ and we get a contradiction. $\square$

4 The proof of the Main Theorem and corollaries

In this section we prove the Main Theorem and other applications of Theorem 3.1.

Proposition 4.1. *Let K be a number field. For every $i = 1, \ldots, n$ let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$ of infinite order. Suppose that the point $R = (R_1, \ldots, R_n)$ in $G = G_1 \times \ldots \times G_n$ is such that G_R is connected. Fix a non-zero integer m. For every $i = 1, \ldots, n$ fix a torsion point X_i in $G_i(\bar{K})$ such that the point $X = (X_1, \ldots, X_n)$ is in $G_R(\bar{K})$. Let F be a finite extension of K over which X is defined. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that for every $i = 1, \ldots, n$ the order of $(R_i - X_i \bmod \mathfrak{q})$ is coprime to m.*

Proof. By Lemma 2.4 the point R is independent in G_R and the point $R' = R - X$ is independent in G_R. Since $G_{R'} = G_R$, by Proposition 2.5 the algebraic group $G_{R'}$ is the product of an abelian variety and a torus defined over K. Apply Theorem 3.1 to R' and find a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R' \bmod \mathfrak{q})$ is coprime to m. This clearly implies the statement. $\square$

Proposition 4.2. *Let K be a number field. For every $i = 1, \ldots, n$ let G_i be the product of an abelian variety and a torus defined over K and let R_i be a point in $G_i(K)$ of infinite order. Suppose that the point $R = (R_1, \ldots, R_n)$ in $G = G_1 \times \ldots \times G_n$ is independent. Fix a finite set S of rational primes. For every $i = 1, \ldots, n$ fix a non-zero integer m_i. Then there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every $i = 1, \ldots, n$ and for every ℓ in S the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{p})$ is $v_\ell(m_i)$.*

Proof. For every $i = 1, \dots, n$ choose a torsion point X_i in $G_i(\bar{K})$ of order m_i and call $X = (X_1, \dots, X_n)$. Let F be a finite extension of K over which X is defined. Call m the product of the primes in S. Apply Proposition 4.1 to R and find a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R - X \bmod \mathfrak{q})$ is coprime to m. Fix $\mathfrak{p}$ as above. Up to discarding finitely many primes $\mathfrak{p}$, for every $i = 1, \dots, n$ the order of $(X_i \bmod \mathfrak{q})$ equals m_i. This implies that for every $i = 1, \dots, n$ and for every ℓ in S the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{q})$ equals $v_\ell(m_i)$. Then up to discarding finitely many primes $\mathfrak{p}$, the ℓ-adic valuation of the order of $(R_i \bmod \mathfrak{p})$ equals $v_\ell(m_i)$ for every $i = 1, \dots, n$ and for every ℓ in S. □

Proof of the Main Theorem. Call n the largest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for all but finitely many primes $\mathfrak{p}$ of K. By Proposition 2.2 we know that n_R divides n. Now we prove that n divides n_R. By Lemma 2.4, $G_{n_R R}$ is connected hence by Proposition 2.5 it is the product of an abelian variety and a torus defined over K. Let ℓ be a rational prime. Apply Theorem 3.1 to $n_R R$ and find infinitely many primes $\mathfrak{p}$ of K such that the ℓ-adic valuation of the order of $(n_R R \bmod \mathfrak{p})$ is 0. Thus there exist infinitely many primes $\mathfrak{p}$ of K such that the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ is less than or equal to $v_\ell(n_R)$. This shows that n divides n_R. Now we prove the second assertion.

Apply Proposition 4.2 to $n_R R$ in $G_{n_R R}$ and find a positive density of primes $\mathfrak{p}$ of K such that for every ℓ in S the ℓ-adic valuation of the order of $(n_R R \bmod \mathfrak{p})$ is $v_\ell(\frac{m}{n_R})$. Because of the first assertion, we may assume that n_R divides the order of $(R \bmod \mathfrak{p})$. Then for every ℓ in S the ℓ-adic valuation of the order of $(R \bmod \mathfrak{p})$ is $v_\ell(m)$. □

By adapting this proof straightforwardly we may remark that n_R is also the largest positive integer which divides the order of $(R \bmod \mathfrak{p})$ for a set of primes $\mathfrak{p}$ of K of Dirichlet density 1.

Lemma 4.3. *Let K be a number field. For every $i = 1, \dots, n$ let G_i be the product of an abelian variety and a torus defined over K. Let H be an algebraic subgroup of $G_1 \times \ldots \times G_n$ such that the projection π_i from H to G_i is non-zero for every $i = 1, \dots, n$. Let ℓ be a rational prime. Then there exists X in $H[\ell^\infty]$ such that $\pi_i(X)$ is non-zero for every $i = 1, \dots, n$.*

Proof. By Proposition 2.5, up to replacing H with H^0 we may assume that H is the product of an abelian variety and a torus. For every $i = 1, \dots, n$ since the projection π_i is non-zero, it is easy to see that there exists Y_i in $H[\ell^\infty]$ such that $\pi_i(Y_i)$ is non-zero. The point Y_1 is not in the kernel of π_1. So if $n = 1$ we conclude. Otherwise let $1 < r \leq n$ and suppose that $\sum_{j=1}^{r-1} Y_j$ is not in the kernel of π_i for every $i = 1, \dots, r-1$. Up to replacing Y_r with an element in $\frac{1}{\ell^\infty} Y_r$, we may assume that for every $i = 1, \dots, r$ either $\pi_i(Y_r)$ is zero or the order of $\pi_i(Y_r)$ is greater than the order of $\pi_i(\sum_{j=1}^{r-1} Y_j)$. Then $\sum_{j=1}^{r} Y_j$ is not in the kernel of π_i for every $i = 1, \dots, r$. We conclude by iterating the procedure up to $r = n$.

Corollary 4.4. *Let K be a number field. For every $i = 1, \ldots, n$ let G_i be a semi-abelian variety defined over K and let R_i be a point on $G_i(K)$ of infinite order. Then for every integer $m > 0$ there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that for every $i = 1, \ldots, n$ the order of $(R_i \bmod \mathfrak{p})$ is a multiple of m.*

Proof. First we prove the case where G_i is the product of an abelian variety A_i and a torus T_i for every $i = 1, \ldots, n$. Call S the set of prime divisors of m. Consider the point $R = (R_1, \ldots, R_n)$ in $G = G_1 \times \ldots \times G_n$. We may assume that $n_R = 1$ by replacing R_i with $n_R R_i$ and we may assume that m is square-free by replacing R_i with $(m/\prod_{\ell \in S} \ell)R_i$ for every $i = 1, \ldots, n$. Since G_R contains R, the projection from G_R to G_i is non-zero for every $i = 1, \ldots, n$ so we can apply Lemma 4.3. Then for every ℓ in S there exists X_ℓ in $G_R[\ell^\infty]$ such that all the coordinates of X_ℓ are non-zero. Write $Y = \sum_{\ell \in S} X_\ell$. By construction Y belongs to $G_R(\bar{K})_{tors}$ and for every $\ell \in S$ the order of every coordinate of Y is a multiple of ℓ. Let F be a finite extension of K where Y is defined. By Proposition 4.1, there exists a positive Dirichlet density of primes $\mathfrak{p}$ of K such that the following holds: there exists a prime $\mathfrak{q}$ of F over $\mathfrak{p}$ such that the order of $(R - Y \bmod \mathfrak{q})$ is coprime to m. Then up to discarding finitely many primes $\mathfrak{p}$ the order of $(R_i \bmod \mathfrak{p})$ is a multiple of ℓ for every ℓ in S and for every $i = 1, \ldots, n$. This concludes the proof for this case.

For every $i = 1, \ldots, n$ let G_i be an extension of an abelian variety A_i by a torus T_i and call π_i the quotient map from G_i to A_i. If $\pi_i(R_i)$ does not have infinite order let R_i' be a non-zero multiple of R_i which belongs to $T_i(K)$. If $\pi_i(R)$ has infinite order then let $R_i' = 0$. Then $(\pi_i R_i, R_i')$ is a K-rational point of $A_i \times T_i$ of infinite order. Clearly for all but finitely many primes $\mathfrak{p}$ of K the following holds: the order of $(R_i \bmod \mathfrak{p})$ is a multiple of m whenever the order of $((\pi_i R_i, R_i') \bmod \mathfrak{p})$ is a multiple of m. Then we reduced to the previous case. $\square$

Acknowledgements

Marc Hindry suggested to me that the greatest integer dividing the order of a point for almost all reductions could be related to the number of connected components of the algebraic subgroup generated by the point. I thank Bas Edixhoven for the idea of imitating Goursat's Lemma in Proposition 2.5. I also thank Brian Conrad and René Schoof for helpful discussions.

References

[1] G. Banaszak, W. Gajda, P. Krasoń, Detecting linear dependence by reduction maps, J. Number Theory 115 (2) (2005) 322–342.

[2] S. Barańczuk, On reduction maps and support problem in K-theory and abelian varieties, J. Number Theory 119 (1) (2006) 1–17.

[3] D. Bertrand, Galois representations and transcendental numbers, in: A. Baker (Ed.), New advances in Transcendence theory (Durham, 1986), Cambridge University Press, 1988, pp. 37–55.

[4] F. A. Bogomolov, Sur l'algébricité des représentations l-adiques, C.R. Acad. Sci. Paris Sér. A–B 290 (15) (1980) A701–A703, presented by J.-P. Serre.

[5] A. Borel, Linear Algebraic Groups, 2nd Edition, Springer-Verlag, 1991, Graduate Texts in Mathematics, 126.

[6] J. Cheon, S. Hahn, The orders of the reductions of a point in the Mordell-Weil group of an elliptic curve, Acta Arith. 88 (3) (1999) 219–222.

[7] A. Grothendieck, Schémas en groupes I: Propriétés génerales des schémas en groupes, Vol. 1 of Séminaire de Géométrie Algébrique du Bois Marie - 1962/64 (SGA 3), Springer-Verlag, 1970, Lecture notes in mathematics 151.

[8] R. Jones, J. Rouse, Iterated endomorphisms of abelian algebraic groups, arXiv:0706.2384 (2007).

[9] C. Khare, D. Prasad, Reduction of homomorphisms mod p and algebraicity, J. Number Theory 105 (2) (2004) 322–332.

[10] E. Kowalski, Some local-global applications of Kummer theory, Manuscripta Math. 111 (1) (2003) 105–139.

[11] D. Mumford, Abelian Varieties, Oxford University Press, 1970.

[12] R. Pink, On the order of the reduction of a point on an abelian variety, Math. Ann. 330 (2) (2004) 275–291.

[13] A. Polishchuk, Abelian varieties, theta functions and the Fourier transform, Cambridge University Press, 2003, Cambridge Tracts in Mathematics, 153.

[14] K. Ribet, Kummer theory on extensions of abelian varieties by tori, Duke Math. J. 46 (4) (1979) 745–761.